STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 08/17)

Fiscal Year	Business Unit	Department	Priority No.
2019-20	2665	California High-Speed Rail Authority	1

Budget Request Name	Program	Subprogram
2665001-BCP-2019-GB	1970 – HIGH-SPEED RAIL ADMINISTRATION	

Budget Request Description
IT Security

Budget Request Summary

The California High-Speed Rail Authority (Authority) requests additional resources to improve the Authority's Information Technology Security Program. The Authority is requesting five (5) permanent positions and $2.23 million in FY 2019-20 and $1.53 million in operating expenses on an ongoing basis. The requested resources will mature the overall security program, including updating policies and procedures, implementing new security solutions, and mitigating security risks and incidents.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed
☐ Yes ☒ No	

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Patty Nisonger	Date 11/19/2018

For IT requests, specify the project number, the most recent project approval document (FSR, SPR, S1BA, S2AA, S3SD, S4PRA), and the approval date.

Project No. Project Approval Document: Approval Date:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By	Date	Reviewed By	Date
Department Director	Date	Agency Secretary	Date

Department of Finance Use Only

Additional Review: ☐ Capital Outlay ☐ ITCU ☐ FSCU ☐ OSAE ☐ CALSTARS ☐ Dept. of Technology

PPBA	Date submitted to the Legislature
Original Signed by Amanda Martin	JAN 10 2019

A. Budget Request Summary

The California High-Speed Rail Authority (Authority) requests additional resources to improve the Authority's Information Technology Security Program. The Authority is requesting resources to address high priority concerns with five (5) permanent positions and $2.23 million in FY 2019-20, and $1.53 million in operating expenses on an ongoing basis. Over a multi-year period, the requested resources will mature the overall security program, including updating policies and procedures, implementing new security solutions, and mitigating security risks and incidents. Funding for this proposal is sourced from the High-Speed Passenger Train Bond Fund.

At present, the Authority's Information Technology (IT) Security staff consists of 2 PYs (an IT Security Specialist and a Network Administrator). The Information Security Officer (ISO) oversees these two positions, in addition to performing duties supporting the Authority's IT infrastructure. The current approach, structure, and staffing level is not adequate to support the Authority's existing enterprise IT solutions and protect the State's information assets. Further, the Authority continues to deploy new business solutions, which also must be secured and supported. This request allows the Authority to establish an Information Technology Security Program as required in the State Administrative Manual (SAM) §5305.

Over a multi-year period, the requested resources will mature the overall security program, including updating policies and procedures, implementing new security solutions, and mitigating security risks and incidents. These resources will improve compliance with: (1) SIMM 5300 Security Framework, established by the California Information Security Office (CISO), (2) the California Information Practices Act, and (3) other state and federal security requirements and standards, such as the National Institute of Standards and Technology (NIST)'s Special Publication 800-53.

Key focus areas include:

- Application Security
- Change and Configuration Management
- Endpoint Security
- Mobile Device Security
- Network Security
- Vulnerability Management
- Contingency Planning
- Security Governance
- Identity and Access Management
- Security Analytics and Monitoring
- Physical Security
- Forensics

A summary of the request is depicted in the table below.

Resources	FY 2019-20	Ongoing (Annual)
Positions	5	5
Personal Services	$704	$704
Operating Expenses	$1,531	$831
Total Dollars	**$2,235**	**$1,535**

The plan for this request includes:

- 5 permanent positions in FY19-20;
- $650,000 for consulting contracts in FY19-20 and $280,000 annually on an ongoing basis;
- One-time software and hardware purchases of $741,000; and ongoing hardware and software maintenance and licensing expenses of $411,000; and
- Ongoing training expenses of $5,000 per position per year.

B. Background/History

Since its inception, the Authority has maintained a business strategy and approach of keeping a lean state staff, while leveraging support from other government entities as well as private sector partners and resources. This approach has generally enabled the Authority to acquire resources as needed, without incurring long-term obligations. The approach has worked well in the engineering and construction components of the Authority's mission. For the Authority's Information Technology program, the approach has also led to aggressive adoption of the state's "cloud-first" vision. To that point, the Authority has adopted the state's shared financial/accounting solution (FI$Cal), utilized the state's email system (Office365), leveraged systems made available by the California Department of Transportation (Caltrans) or other departments, and deployed unique systems via vendor-hosted solutions.

The Authority has also maintained a small IT program, totaling 15 civil service employees, with only 2 positions focused on network and information security, augmented by 2 vendor FTEs. This level of support is no longer adequate and presents a significant risk to the Authority's operations and assets. The need for additional dedicated IT security resources has grown due to the following:

- Additional business systems have been deployed (e.g., cost management system, contract management system, risk management system);
- Increased complexity of Authority systems that are integrated and share critical data across domains, networks, and external service providers;
- The number of supported users (state and vendor staff) has increased as the overall construction program has grown;
- Evolving state and federal requirements and standards; and
- Evolving security threats, including cyber-attacks from foreign nations.

A recent assessment by the California Military Department, along with internal reviews of standards and practices, have identified high risk security vulnerabilities and compliance matters. These vulnerabilities expose the Authority to security risks that threaten to:

- Disrupt productivity and interfere with the timely delivery of the nation's first high-speed rail system;
- Expose and/or compromise critical and/or sensitive data, including proprietary information, confidential information, financial data, and personally identifiable information protected by state and federal laws; and
- Damage the reputation and public trust of the Authority.

The California Department of Technology (CDT) established the Information Security Foundational Framework in November of 2017. Consistent with the National Institute of Standards and Technology (NIST), this framework sets objectives for compliance that protect information assets and address organizational risk. This proposal requests resources and funds to help the Authority meet the requirements of this framework.

C. State Level Considerations

This request supports a key objective identified in the California High-Speed Rail Authority 2016 Business Plan and re-affirmed in the 2018 Business Plan: "Initiate high-speed rail services in California as soon as possible". As additional IT solutions and infrastructure (including mobile devices and additional physical sites) are being deployed to support construction in the field, our Information Technology Network and Security team need to be able to identify potential network outages due to cyber security threats before they occur, reducing downtime and alleviating scheduling concerns.

Moreover, this proposal directly supports the California Department of Technology's "Vision 2020" goal of "Ensure Secure Delivery." With the requested resources, the Authority's IT Security Program will be better equipped to develop vital, effective programs required to meet the California Technology Strategic Plan priorities, facilitating the following initiatives: enhanced protection of California's technology assets, development of a collaborative inter-departmental security risk reduction strategy, and improvements to mission critical security capabilities. In addition, this proposal will support the

Authority's ability to mature their security capabilities in response to the high-risk findings from the California Military Assessment.

D. Justification

The State Administrative Manual (SAM) §5300, released by California Information Security Office (CISO), provides a security and privacy policy framework that state entities must follow. The CISO also requires adherence to the National Institute of Standards and Technology (NIST)'s Special Publication 800-53, which is designed to facilitate compliance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance. The Authority requires staff, consulting assistance, and tools to meet the requirements of these state and federal security policies.

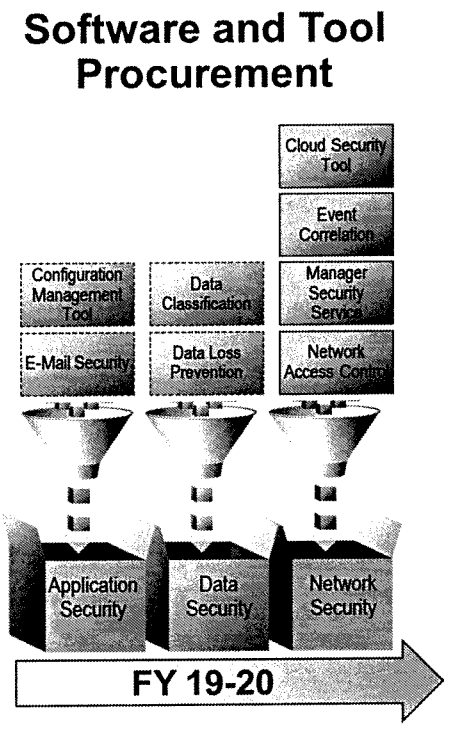
The requested resources will significantly improve the Authority's security posture by:

1) Developing and implementing policies, procedures, and technologies that improve compliance with CDT's Security Foundational Framework;
2) Creating and maintaining data security and governance programs;
3) Continuously scanning for vulnerabilities and resolving network faults; and
4) Establishing and maintaining a data loss prevention program.

To ensure the Authority's Information Security Officer (ISO) can better focus on creating and maintaining a proper IT security program, this request will add one (1) supervisor (IT Supervisor II) to oversee day to day network and security operations, two (2) IT Security Professionals (IT Specialist II), and two (2) IT Security/Network Administrators (IT Specialist I).

Staffing alone will not be sufficient to ensure security compliance. Tools that monitor, analyze, mitigate, and report on IT security risks are required to protect the Authority's network, systems, and data. Implementation of these tools will be initiated in FY19-20; mapped to address priority findings in the Military Security Assessment; planned so as not to overburden staff with software implementation work while they perform their day-to-day tasks; and organized to best fit with the level of anticipated staff skills (e.g., more technical, complex software would be procured later, allowing for staff to first acquire sufficient skills and knowledge to be effective users).

The figure below provides a high-level overview of the IT Security Tools that will be procured and implemented by the Authority's Information Technology Security Program:



The following summarizes the requested operating expense funding:

- Tools (Software/Hardware) – Estimated to be $741,000 for one-time acquisition costs, and $411,000 ongoing for software licenses and maintenance. Software products will be procured that will enable security staff to proactively monitor and correlate information from various information sources, identify security vulnerabilities, and track remediation efforts over time.
- Training – Estimated to be $5,000 per person annually, based on the Authority's experience with similar training needs (each person taking 1 or 2 classes per year at a cost of $2,500 - $5,000 per class) to keep current with new threats, technologies, and security solutions. Threats and compliance standards are continuously shifting, requiring the Authority's IT Security Team to stay current with training and recertification efforts.
- Consulting Services – Estimated at $650,000 in FY19-20 and $280,000 per year thereafter. Consulting services include on-site consultants (Security Architects) to augment permanent state staff. The staffing approach will utilize consultant expertise to support tool implementations and provide initial expertise and training to permanent staff as they are hired. Ongoing consultant support will be used to ensure tools are optimized and policies or programs continually mature to protect against new and emerging threats. On-site consultants will be reduced as state staff gain experience and training.

This request enables the Authority to make substantial improvements and address the priority security objectives outlined in the California Department of Technology (CDT), Office of Information Security's SIMM 5300-B Foundational Framework. As the Authority's IT Security Program improves compliance with the foundational framework objectives, they will continue to address other applicable control areas to protect information assets and address organizational risk.

Consequences of Not Receiving the Requested Resources

The information processing and information assets used at the Authority are critical to the delivery of the nation's first high-speed rail service. Information technology systems play a vital role in planning, designing, building, and operating this program in the state.

Without these requested resources, the Authority will continue to be vulnerable to cybersecurity incidents. A targeted cyberattack could result in compromise and damage to the state of California and the high-speed rail project. In addition, without these requested resources, the Authority will be:

- Increasingly exposed to severe damages resulting from cybersecurity events;
- Unable to adequately protect the state's resources;
- Unable to achieve the required compliance with state, federal, and other IT security mandates; and
- Unable to address the mandates of Information Practices Act, as directed by the state and federal privacy mandates.

E. Outcomes and Accountability

If this request is approved, the Authority will be able to implement mission critical security tools to increase the protection of critical information system assets that support the delivery of the first high-speed rail system in the nation and to:

1) Take recommended steps to address documented critical and high-risk findings in information technology security assessments thus mitigating the Authority's exposure to data breach related lawsuits.
2) Significantly improve the Authority's cybersecurity posture by adding to the tools that IT has available to identify, protect, detect, and respond to cybersecurity attacks as recommended in state and federal cybersecurity mandates.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve five (5) permanent positions and $2.23 million in High-Speed Passenger Train Bond Funds to enhance the Authority's Information Technology Security program.

Analysis of Alternative 1: This alternative uses a combination of internal and external resources to remediate information technology security risks and vulnerabilities identified in both internal and external assessments, protect the state's resources and data, and increase the Authority's compliance with mandatory security and privacy directives.

Pros:

- Enhances the Authority's ability to detect, prevent, and protect itself and its data from cybersecurity attacks;
- Increases the Authority's compliance with state and federal mandates;
- Improve, create, and sustain planned future IT Security Program upgrades (including network enhancements);
- The Authority will retain and enhance staff experience and skill in aggregate logging, enterprise security monitoring, and remediation;
- Outsourcing vendor(s) will be experienced with aggregate logging, enterprise security monitoring, and remediation programs; and
- Allows the organization to address the progress and maturity of the security program and address additional staffing and other expense needs in a future BCP.

Cons:

- Creates additional ongoing operating expenses.

Alternative 2: Approve $1.26 million in consulting services and $1.152 million in one-time and ongoing costs to enhance the Authority's Information Technology Security program.

Analysis of Alternative 2: This alternative relies on consulting services rather than civil service positions to remediate information technology security risks and vulnerabilities identified in multiple assessments, protect the state's resources and data, and bring the Authority into compliance with mandatory security directives. Consulting services estimated at $1.8 million including on-site consultants (Security Architects) in place of permanent state staff, at a rate of

approximately $30,000 per consultant per month. The anticipated workload of 5 permanent fully trained staff would be supplemented with five (5) consultant FTEs. An additional $741,000 in one-time and $411,000 in ongoing costs will include the implementation and licensing costs for the security tools and hardware.

Pros:

- Enhances the Authority's ability to detect, prevent, and protect itself from cybersecurity attacks;
- Increases the Authority's compliance with state and federal mandates;
- Improve, create, and sustain planned future IT Security Program upgrades; and,
- Outsourcing vendor(s) will be experienced with aggregate logging, enterprise security monitoring, and remediation programs.

Cons:

- Authority will be dependent on the outsourced vendor for its internal IT Security Program;
- Outsourced vendor(s) will not be as experienced with the Authority's environment as Authority employees would be;
- Outsourcing will still require Authority personnel for management and oversight of the vendor relationship(s) and performance, and require additional contract management responsibilities and skills;
- Over a longer-period, outsourcing will cost more to achieve the same level of performance and service that can be provided by Authority employees;
- Authority will not retain and enhance staff experience and skill in mandated data privacy and some cybersecurity compliance functions;
- Vendors are often less experienced with specific state and federal regulations and requirements, including those mandated by CDT; and creates an ongoing operating expense.

Alternative 3: Deny this request.

Analysis of Alternative 3: This alternative is not viable given that the Authority's IT Security Program is not in compliance with state and federal standards. Additional staff with appropriate security expertise and appropriate tools to ensure data and resources are secure are critical to achieving compliance.

Pros:

- Will not increase Proposition 1A administrative expenditures.

Cons:

- The Authority will remain at risk for security incidents and out of compliance with state and federal security mandates.

G. Implementation Plan

July 1, 2019

H. Supplemental Information

None

I. Recommendation

The Authority recommends the approval of Alternative 1: five (5) permanent positions and $2.23 million appropriation in High-Speed Passenger Train Bond Fund to enhance the Authority's Information Technology Security Program.

BCP Fiscal Detail Sheet

BCP Title: IT Security

BR Name: 2665-001-BCP-2019-GB

Budget Request Summary

	FY19					
	CY	BY	BY+1	BY+2	BY+3	BY+4
Personal Services						
Positions - Permanent	0.0	5.0	5.0	5.0	5.0	5.0
Total Positions	**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**5.0**
Salaries and Wages						
Earnings - Permanent	0	450	450	450	450	450
Total Salaries and Wages	**$0**	**$450**	**$450**	**$450**	**$450**	**$450**
Total Staff Benefits	0	254	254	254	254	254
Total Personal Services	**$0**	**$704**	**$704**	**$704**	**$704**	**$704**
Operating Expenses and Equipment						
5301 - General Expense	0	10	10	10	10	10
5302 - Printing	0	5	5	5	5	5
5304 - Communications	0	15	15	15	15	15
5320 - Travel: In-State	0	5	5	5	5	5
5322 - Training	0	25	25	25	25	25
5324 - Facilities Operation	0	40	40	40	40	40
5340 - Consulting and Professional Services - Interdepartmental	0	650	280	280	280	280
5344 - Consolidated Data Centers	0	25	25	25	25	25
5346 - Information Technology	0	5	5	5	5	5
5368 - Non-Capital Asset Purchases - Equipment	0	741	411	411	411	411
539X - Other	0	10	10	10	10	10
Total Operating Expenses and Equipment	**$0**	**$1,531**	**$831**	**$831**	**$831**	**$831**
Total Budget Request	**$0**	**$2,235**	**$1,535**	**$1,535**	**$1,535**	**$1,535**

Fund Summary

Fund Source - State Operations						
6043 - High - Speed Passenger Train Bond Fund	0	2,235	1,535	1,535	1,535	1,535
Total State Operations Expenditures	**$0**	**$2,235**	**$1,535**	**$1,535**	**$1,535**	**$1,535**
Total All Funds	**$0**	**$2,235**	**$1,535**	**$1,535**	**$1,535**	**$1,535**

Program Summary

Program Funding						
1970 - High-Speed Rail Authority--Administration	0	2,235	1,535	1,535	1,535	1,535
Total All Programs	**$0**	**$2,235**	**$1,535**	**$1,535**	**$1,535**	**$1,535**

BCP Title: IT Security **BR Name: 2665-001-BCP-2019-GB**

Personal Services Details

Positions	Salary Information Min	Mid	Max	CY	BY	BY+1	BY+2	BY+3	BY+4
1402 - Info Tech Spec I (Eff. 07-01-2019)				0.0	2.0	2.0	2.0	2.0	2.0
1404 - Info Tech Supvr II (Eff. 07-01-2019)				0.0	1.0	1.0	1.0	1.0	1.0
1414 - Info Tech Spec II (Eff. 07-01-2019)				0.0	2.0	2.0	2.0	2.0	2.0
Total Positions				**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**5.0**

Salaries and Wages	CY	BY	BY+1	BY+2	BY+3	BY+4
1402 - Info Tech Spec I (Eff. 07-01-2019)	0	161	161	161	161	161
1404 - Info Tech Supvr II (Eff. 07-01-2019)	0	99	99	99	99	99
1414 - Info Tech Spec II (Eff. 07-01-2019)	0	190	190	190	190	190
Total Salaries and Wages	**$0**	**$450**	**$450**	**$450**	**$450**	**$450**
Staff Benefits						
5150900 - Staff Benefits - Other	0	254	254	254	254	254
Total Staff Benefits	**$0**	**$254**	**$254**	**$254**	**$254**	**$254**
Total Personal Services	**$0**	**$704**	**$704**	**$704**	**$704**	**$704**